Cyber Security Policy

Public

Approved by ELT, 13 March 2026

1 Purpose

The purpose of this Cyber Security Policy is to define the technical and organizational measures required to protect NG Nordic's information, systems, and critical services.

This policy supports and expands the high-level Information Security Policy and ensures compliance with the NIS 2 Directive, applicable national legislation, and recognized industry standards.

Each section in this policy may be supported by additional topic specific policies, procedures, guidelines and records as separate documentation.

2 Scope

This policy applies to:

- All NG Nordic business units and locations
- All employees, contractors, and third parties with access to NG Nordic systems
- All information systems, operational technology (OT), cloud environments, and IT services used by NG Nordic.

3 Responsibilities

Responsible function for support and implementation of this policy

Group IT & Security function is responsible for the governance and management practices for developing, guiding, and supporting information security and cyber security initiatives at a Group level.

Other key roles and responsibilities:

Executive Management: Provide leadership and support for information security initiatives, allocate resources, and ensure compliance with this policy.

Leaders/Managers: Ensure that employees in their area of responsibility follow cybersecurity guidelines, complete assigned training and carry out relevant processes in accordance with this policy. Managers are also expected to promote a culture that supports cybersecurity.

Chief Information Security Officer (CISO): Oversee the development, implementation, and maintenance of the security controls in this policy, and serve as the primary point of contact for information security matters.

Group IT: Enable and support secure operations across NG Nordic by implementing and enforcing the technical and operational controls defined in this policy.

All Employees: Comply with this policy, standards, and security requirements. Use IT systems responsibly and report incidents, risks, or non-compliance.

4 Risk Management

NG Nordic shall maintain a structured risk management process that includes:

- Annual information security risk assessments
- Risk acceptance criteria and documented treatment plans
- Evaluation of risks related to digital operations, supply chain, OT, and cloud environments
- Continuous monitoring of emerging cyber threats

Risk assessments must be documented and reviewed by Group IT & Security.

5 Asset Management

NG Nordic must maintain an accurate inventory of:

- Hardware assets
- Software, applications, and SaaS services
- IT, IoT and OT equipment
- Data assets and classifications
- External service providers and connections

All assets must have an owner, a defined classification, and documented protection requirements.

6 Access Control

NG Nordic enforces strict access control principles:

- Least privilege and need-to-know basis
- Strong Multi-factor authentication for privileged and remote access
- Continuous authentication solutions, such as Single-Sign-On (SSO)
- Role-based access control (RBAC)
- Regular access reviews
- Immediate revocation of access during offboarding

Default-deny access models must be implemented where supported.

7 Identity Management

All identities - human, application, and machine accounts–must be uniquely identifiable.

Password requirements, lifecycle controls, and secure credential handling must be enforced through centralized identity and access management (IAM) systems.

8 Network and System Security

NG Nordic implements a layered network and system defenses, including:

- Network segmentation for IT and OT based on Purdue model
- Firewalls and secure gateways
- Zero-trust principles for secure remote access
- Hardening of endpoints, servers, and cloud environments
- Secure configuration management

Changes to critical systems must follow an approved change management process.

9 Logging, Monitoring, and Detection

NG Nordic shall maintain logging and monitoring capabilities appropriate to system criticality:

- Centralized log collection
- Minimum log retention of 12 months for security logs
- Monitoring of critical assets and privileged accounts
- Automated alerting for security events
- Integration with SIEM/SOC services
- 24/7 SOC services for all critical IT and OT systems

Logs must be protected against tampering and unauthorized access

10 Incident Handling and Reporting

NG Nordic maintains an Incident Response Plan (IRP) covering:

- Detection, triage, containment, eradication, and recovery
- Communication, forensics, and evidence preservation
- 24/7 reporting channels
- Escalation procedures based on impact

NIS 2 regulated incidents must be reported according to the NIS 2 notification procedure to authorities within 24 hours.

All employees must report suspected incidents immediately to IT Support.

11 Business Continuity and Disaster Recovery

NG Nordic maintains business continuity and disaster recovery plans (BCP/DRP) that include:

- Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
- Regular testing of backups and failover procedures
- Secured and immutable backups stored offsite or in isolated cloud environments.

System owners of critical systems must ensure continuity measures are implemented.

12 Vulnerability and Patch Management

NG Nordic must:

- Continuously identify and mitigate vulnerabilities
- Track exposures to critical IT and OT systems
- Apply security patches within defined timelines
- Critical security patches must be implemented as soon as possible
- Conduct periodic vulnerability scans and penetration testing
- Refrain from utilizing End-Of-Life components.

Unpatched high-risk vulnerabilities must be escalated to IT Security.

13 Secure Development (SDLC)

NG Nordic must enforce a secure development lifecycle that at minimum includes:

- Secure coding guidelines
- Code reviews and automated scanning
- Security testing of developed software
- Management of software bills of materials (SBOM)
- Secure API and integration controls

14 Supplier and Supply Chain Security

NG Nordic evaluates supplier security through:

- Pre-contract security assessments
- Minimum security requirements in IT and OT related contracts
- Ongoing monitoring for critical suppliers
- Obligations for incident notification and cooperation

Suppliers handling critical services must align with NIS 2 requirements.

15 Cryptography and Key Management

NG Nordic must apply secure cryptographic practices:

- Approved algorithms and key lengths
- Encryption of data in transit and at rest
- Secure key storage, rotation, and revocation
- Management of certificates and secrets

16 Training and Awareness

NG Nordic maintains a cybersecurity training program including:

- Regularly Phishing simulation tests and security awareness material
- Mandatory annual IT security awareness training
- Role-specific technical training for IT and OT personnel
- Executive and Board cybersecurity education

Completion of training must be monitored and enforced. Managers are responsible for ensuring their employees follow mandatory training.

16 Compliance and Effectiveness Assessment

NG Nordic shall perform regular assessments to ensure compliance, by:

- Internal checks or audits
- Technical security testing
- Control maturity assessments
- Reporting of nonconformities and remediation requirements

Results are reviewed by the CISO and reported to executive management and to the Board.

Location and process	Head office / IT / Information Security	**Document category**	Policy
Last approved date	20/03/2026 (Ole Martin Refvik)	**Next revision date**	13/03/2027
		Document responsible	Ole Martin Refvik

5 Review cycle

This policy is reviewed on an as-needed basis. Any amendments to this policy require approval by ELT.